Jori Kymäläinen

IMPLEMENTING TWO-FACTOR AUTHENTICATION

Degree Programme in Information Technology

2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

IMPLEMENTING TWO-FACTOR AUTHENTICATION

Kymäläinen, Jori
Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2018
Number of pages: 33
Appendices: 1

Keywords: mfa, authentication, two-factor, VPN, SAMK

Two-factor authentication is a part of modern authentication technologies. It is also called multifactor authentication or shortly 2FA. Traditional one-factor authentication method process provides only one factor, typically a password. This is quite easy possible to hack. Two-factor authentication is based in the assumption, that two of the three factors of authentication are used.

Satakunta University of Applied Sciences, later called SAMK, operates with modern ICT environment. Administrative portals and management systems needs better security. To find the best possible way is to implement secure two-factor authentication method and bring it to production use in SAMK environments. At least more complex authentication is needed with administrative systems, but the solution must be implementable also to whole staff everyday use e.g. with VPN. A first pilot environment will be made and after that the solution can be extended to heavier use.

The research type used will be case study research. That research type will be best suitable to match any needs of the wanted solution.

The most benefit for this thesis is Satakunta University of Applied Sciences, it will get a modern secure authentication layer for its systems and get documentation how it will work and need to be published. This is really needed in SAMK environment so benefit for the company will be good. The thesis will include two-factor authentication methods, use in on premise environment, use in cloud systems and different usage surveys and doing the implementing action in SAMK environment.

CONTENTS

1 INTRODUCTION

Authentication means, that the identity of the user or service is authenticated when logging on to a service. The traditional way of authentication has been to use one-way authentication where a username and password are required. This method is still very common in most web services and ICT environments. One-way authentication is also susceptible to abuse and data hacking, because a hacker has many ways to capture the user name and password with modern hacking technologies. The most common way is to send phishing messages.

Satakunta University of Applied Sciences operates with modern ICT environment. Administrative portals and management systems needs better security. Staff and student use SAMK systems remotely and their connections should also be more secure. Normally security is handled with long and complex passwords and may need to be changed often. This is laborious. There´s a need to get more secure authentication method to user logons and remote use. One way to raise the security is to use two-factor (of sometimes maybe three-factor) authentication. There are different solutions and ways to implement this method, but the best solution or solutions to do this must be researched and tested in SAMK environment.

What would be the best way to find a secure two-factor authentication method and bring it into production in SAMK environment? At least more complex authentication is needed with administrative systems, but the solution must be implementable also to whole staff everyday use e.g. with VPN. First making a pilot environment and after that the solution can be extended to heavier use.

The most benefit for this thesis is Satakunta University of Applied Sciences, it will get a modern secure authentication layer for its systems and get documentation how it will work. This is really needed in SAMK environment so benefit for the company will be good. The thesis will include two-factor authentication methods, use in on premise environment, use in cloud systems and different usage surveys and doing the implementing action in SAMK environment. Three-factor authentication or other more complex methods will be excluded, centralizing to two-factor authentication will be

the important thing and it is the method what is wanted to be used in SAMK. The purpose is to explore and implement a new, secure way to take into production in SAMK ICT environment.

The research type will be case study. During the research, the status of the environment is mapped and the organization´s security manager will be interviewed to gain an insight into the organization´s expectations of research and its results. As the author of this thesis works in the SAMK ICT environment, he also has a personal view of the organization´s present status. The organization already has a light experience of using multifactor authentication, but now it is to be expected to a deeper and versatile use. Based on the experience gained in the research, it is expected to take multifactor authentication into more widely production in SAMK environments. A consideration how well the results of this case study could be utilized e.g. in another university of applied sciences is finally done.

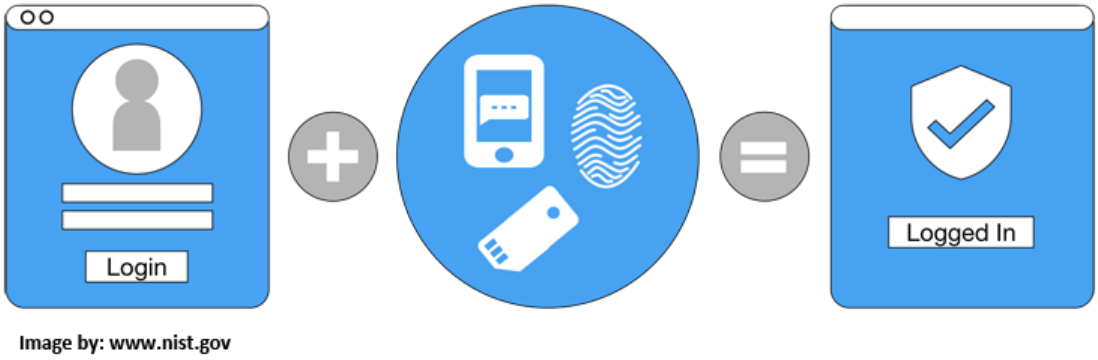
As part of this process, setup documentation is also generated and will be shown in appendices.

2 ABOUT 2-FACTOR AUTHENTICATION

2.1 General

Two-factor authentication is a part of modern authentication technologies. It is also called multifactor authentication or shortly 2FA. Traditional one-factor authentication process provides only one factor, typically something on what an individual can memorize. Personal numbers (PIN) and passwords are typical examples of this kind of authentication methods. Two-factor authentication needs more challenge from the individual. This authentication is based in the assumption that two of the three factors of authentication are used. They are:

- **Something you know**, this is the simple-based authentication and most common type. User must remember a string of characters and present them to a system. The characters are reused many times. This type is most vulnerable to attacks, especially to guessing attacks.
- **Something you have**, this authentication requires some form of physical token. This can be a USB stick, mobile phone or password booklet. After user logs on to a service with a password, a code is sent via SMS or mobile application and after putting the code to the challenge, user can continue logging. Banks and government-based web-services in Finland are using this kind of authentication widely.
- **Something you are**, some biometric thing e.g. Your fingerprint, iris scanning, voice analysis and so on. Biometric authentication is not like the other types, because it does not rely on secrets. Biometrics are not secrets, but they rely on registering and later matching what are believed to be distinguishing physical or behavioural characteristics of individuals. (Millett, 2003, ss. 104-124)



Picture 1: 2-factor authentication (U.S. Department of Commerce, 2018)

2-Factor authentication is not a new technology. Bank world have used 2-factor-based technology in modern networks since 90´s. When people use a credit or debit card and they need to enter the PIN code, that is an example of 2-factor authentication. Authentication based on the "something you know" and "something you have" is commonly used in banks and public services and recently many ordinary e-mail services have offered this for optional method to logging in. This way is also strongly recommended by the hardware and software manufacturers. 2-factor authentication and modern techniques are growing fast especially in cloud services, because it´s quite easy to put it in use vs. legacy networks. Biometric recognition "something you are" is needed for example in access to data centres. To get in to a data center you may need to enter a passcode and fingerprint to outer door. Inside the centre there may be user other combinations of authentication, maybe passcode and a hardware token. In high security environments, two people may be needed to open a door. They must do biometric detection at the same time to allow access to a room. In this case a single person can´t enter the room individually. Banks may use 3- or even 4-factor authentication, because it´s more secure.

2.2 Common ways to use 2-factor authentication

2.2.1 SMS message to mobile phone

SMS is a common authentication method. The user logs on to a service by entering his own login information and after that the service sends code in a text message to user´s mobile phone. User enters the code to the 2-factor logon screen and can continue

to service. This method is commonly used for example to reset the password of e-mail portals and to log on to some services.

2.2.2 Multifactor authentication app

It is also possible to use a separate authentication application that can be downloaded to a smartphone. These applications vary depending on the manufacturer. Microsoft´s Authenticator application can handle different roles. It may be in the notification mode and the application warns user when the user is signing in to a service and the user must accept or reject a request. Another option is to use the verification code, which when the user enters the ID and password, must also fetch the code entered in the Authenticator application and enter it into the login field.

2.2.3 Authentication with USB stick

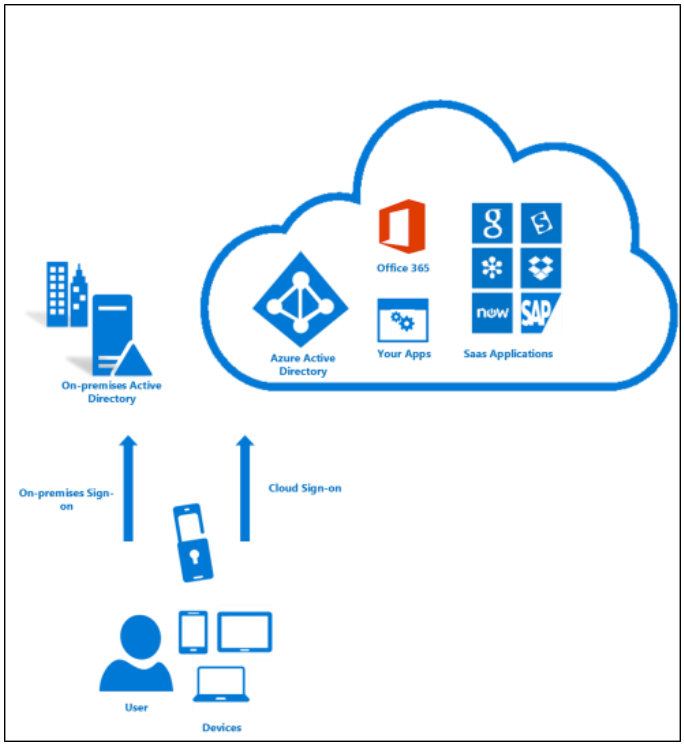
There is a possibility to use a USB stick for additional authentication. In this case user do not need to enter any separate code himself, but the USB stick manages this session. One of the popular two-factor authentication sticks are made by Yubikey (www.youbico.com). When logging in to a computer and services, the usb stick is fed to a computer and it handles the 2-factor part of the authentication. This stick is also supported by popular password managers such as LastPass and DashLane and many popular services as Facebook, Dropbox and Citrix.

2.3 2-factor authentication recommendations in business environments

2.3.1 Microsoft Azure / Office365

Microsoft´s secure login behaviors are marked with recommendation of two-step authentication when signing in to the Azure cloud environment and it´s services or the Office365 portal. Two-step authentication should be turned on at least to service administrator logins. Is this option enabled or not, it will affect the Microsoft Office365 Secure Score level. If two-step authentication is not enabled to administrators, this

score calculator will warn it immediately. If wanted, this authentication can be extended to all users. Administrator can enable two-step authentication without extra costs and it can be done directly from the admin portal. For certain users and application, authentication can be turned on for additional work and authentication will cost based on the number of signups.



Picture 2: Azure 2-factor authentication (Microsoft Corporation, 2018)

Azure two-step authentication has several pricing types depending on model. Volume licensing price is not shown, but in North Europe per-user consumption-based billing with unlimited authentications costs 1.181€ per month. If Satakunta University of Applied Sciences would enable two-step authentication to Office365 services and no volume licensing option would be used, the pricing could look like this:

- Staff only (400 members): 472,4 euros per month.
- Staff and students (400 staff + 6000 students): 7558,4 euros per month.

The list price per month is quite high even if only staff were selected. Volume licensing option may bring some discount, but it goes without saying, that it is not possible for students to take this option with these costs. The second factor can also be other than

SMS or mobile phone, because in school world you cannot ask phone number from a minor child. Some token device could be the answer to this.

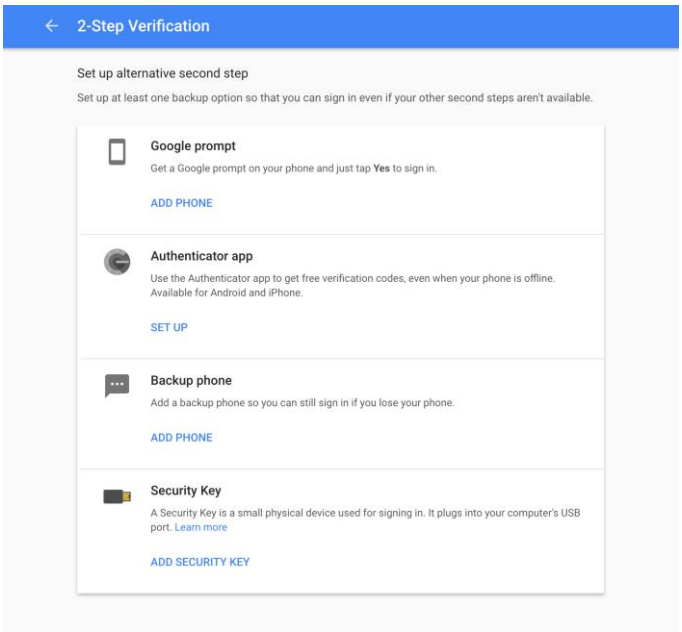
2.3.2 Amazon Web Services

Amazon Web Services (later AWS) supports multi-factor authentication as a simplest best practice to access login to sign in to an AWS website. Multifactor authentication (MFA) can be turned on to administrators and for individual users, who have been created under AWS account. Authentication can also be used to control access to AWS service APIs. Using the virtual MFA device (usually smartphone and app like Google Authenticator or Authy 2-Factor Authentication) the use of MFA is free. AWS does not support accepting new participants for the SMS MFA preview, so new accounts must use either hardware or virtual MFA devices. Amazon offer several devices for international customers like Hardware key Fob MFA Device or Hardware Display Card MFA Device, these are offered by a third-party provider. They cost $12.99-$19.99 depending on the technology.

Picture 3: AWS Multi-Factor Authentication (Amazon Web Services, 2018)

2.3.3 Google Cloud

Google Cloud also recommends and offers possibility to configure 2-step verification for its accounts. This can be done with SMS, Google Authenticator Mobile app or hardware security keys provided by FIDO U2F. Google recommends using the FIDO security key as it brings the strongest security. FIDO security key costs at amazon.de marketplace 24,99€ per key. Google seems not to take extra cost when using extra verification so the possible cost is coming if hardware keys are purchased.



Picture 4: Google Cloud 2-step Verification (Google inc., 2018)

2.4 Challenges

Multifactor methods are not absolute secure. 2-factor authentication is also available to be hacked. Hackers have found a way to obtain the codes needed for 2-factor authentication. Based on reports from the NSA, at least Russian hackers have used a way to attract a user directly to a genuinely impressive web page where user ID and password are being asked. If user is using 2-factor authentication, the site also asks user to enter his security code that was sent to the phone. By this method Russian hackers have managed to break Google´s 2-factor authentication. Once the user has entered their personal information and phone security code, the site sent the user to

genuine Google service. The users maybe never noticed, that their authentication information had been stolen. (Komonen, 2017)

The hackers must acquire the physical component of the log-in or must gain access to cookies or tokens placed the device by the authentication mechanism. This can be done with a phishing attack (one example was presented above), malware or credit card skimming. When USB stick or mobile phone is used for 2-factor authentication, this method is weak if the device is lost or stolen. The user needs the device to reset or change their password or ID. Nowadays there are some ways how to do things in management programs if the device is missing. The account recovery is also a problem, that is not adequately solved. Account recovery can work as a tool for breaking 2-factor authentication, because it will bypass 2FA. E.g. in Google if creating an account and then pretend to lose data, account recovery will take extra time, but several days later Google can disable account´s 2FA and after that it is possible to log on with the account without 2FA. Duo Security´s Oberheide tested this in 2015.
(Rosenblatt & Cipriani, 2015)

There is a risk that hardware token and password is stored in same place and they will get stolen at the same time. You could say, that all security instructions tell you to keep these passwords and token in different locations, but some people violate these rules because they do not either remember all the needed passwords or feel the usability difficult.

In some cases, same authentication software settings can be configured on multiple devices. When the hacker gets a user ID and password, he or she can use the second device to obtain the security code required for authentication. (Thomson, Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication, 2018)

One challenge is user experience. Users experience extra authentication as cumbersome, hindering the user experience. As a result, people are pretty much protecting their Google accounts very badly. Google engineer Grzegorz Milka recently told, that only 10% of Google users have connected two-factor authentication when using the service. Of those using the service, 10% had reported that they had difficulties entering

the code keys received on their mobile phone. (Thomson, Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication, 2018)

3 CASE SATAKUNNAN AMMATTIKORKEAKOULU

3.1 The research

The type of this research will be case study research. Case study is the predominant approach of qualitative research in business economics and will examine one or multiple cases. Information is obtained through surveys, interviews, observation and use of archive material. The case may be descriptive, theory-based or theory-making. The research is attached to understanding and solving the case. Some examples of this type of research is to process a new technology or process a strategic change in an organization.

Case studies can serve different purposes. Case study needs to be explained. There may be only a few cases before the investigation, and after the investigation, the case can be explained more widely, e.g. as a case that supports the investigated case. Case studies are suitable for small-scale studies and researchers often have experience of a case to be investigated, and the study wants to explain what´s happening in this context. (Hammond, 2013)

In the case of Satakunta University of Applied Sciences the aim is to find a suitable solution for 2-factor authentication initially to administrative systems and possible expand it to cover other systems used by whole staff. During the research an interview with the university´s IT security officer will be done to explore expectations and wishes for the case. Because some of the services in the university area are already available for 2-factor authentication, these areas are not affected. The purpose is to find out and build 2-factor authentication in an environment where it can be implemented with own tools and a service provider. A test environment will be built and configured to match production environment. At the end of the implementation the future will also be considered and the related challenges.

3.2 The environment

In Satakunnan ammattikorkeakoulu, in English Satakunta University of Applied Sciences (later SAMK) many administrative ICT systems are used and there are different ways to authenticate to the system administration portals. The common will is to require more secure authentication method for maintenance measures. In some cloud services we already use two-factor authentication, which is implemented by third-party software. Currently end-users do not use two-factor authentication on SAMK systems by SAMK ICT and this feature is not planned to be released recently. The need for a stronger identification in the management of the core systems of SAMK will be implemented by use of local hardware.

Interview with Osmo Santamäki, the ICT Security Manager of SAMK´s thoughts about authentication methods in SAMK environments. The interview has been conducted as an open interview, where the current authentication situation and the wishes of 2-factor authentication is explained and some discussion how authentication would be developed in the future.

“Identity management is well under control in SAMK. Identities are being generated and deleted automatically. There are some exceptional systems, but they are left out during system updates. In these exceptional cases, the identities are entered manually. There are four kind of authentication methods: AD, AD synchronization, ADFS and HAKA AD authentication, which is also used through the RADIUS service. HAKA authentication will include two-step authentication by the operator. This service is already in trial mode.” (Santamäki, 2018)

“With two-step authentication is being sought for a better level of security. The common risk to lose passwords into the hands of outsiders due to data breach, neglect, hacking or malicious activity. Two-step authentication is a great improvement. It is impossible to divide account data to other people. Universal accounts are also disabled.” (Santamäki, 2018)

What do you expect from this case?

“I look forward to find a solution for two-step authentication to VPN connections. This is to be implemented for remote management authentication. It is assumed that the solution uses the RADIUS service and that service can also be used for authentication in other systems. An important part is also the documentation of the solution. A successful solution requires the implemented and documented two-step authentication of remote management VPN” (Santamäki, 2018)

“In the future we strive to focus on HAKA authentication and include increasingly more services to it. The most problematic is AD synchronization, because the passwords are copied to external system. It is hoped that this system will be eliminated soon as possible through system reforms. The near time goal is to enable two-step authentication in all remote management connections. In the longer term, we strive for a solution in which the method of logging is identified and then is concluded, if two-step authentication is needed or not. This means, e.g. that when user is signing in for the first time, it is performed in two steps and when using the same device, there is no need for two steps. Device replacement will enable the two-step authentication again.” (Santamäki, 2018)

3.3 Choosing the technology

In SAMK there have been some small testing with MFA software called DUO Mobile. Usage testing has not been done with Active Directory-based use, but the users have been local accounts in local systems. DUO Mobile is free for small and test use and can be easily increased to more and more users by several licensing options. Because the free use it is easy to implement with SAMK special use and for testing purposes.

“When a user tries to access an application, the first step of DUO´s trusted access platform is to confirm that user´s identity with two-factor authentication (2FA) and contextual user access policies. This ensures they are who they say they are and whether they´re permitted to access their desired application”. (Duo Security Inc., 2018)

Duo´s 2FA solution requires users to carry only one device, their mobile phone. The simplest way to use Duo is to install DUO mobile application to phone and use DUO Push or U2F (hardware device, such as USB). DUO also supports many technologies to implement for 2-factor authentication. These are:

- **Push notification**; verifying identity against mobile app or wearable device, like smart watch.
- **Security tokens**; a hardware token which can generate passcode which user must type to a two-factor prompt.
- **SMS passcodes**; the standard way. Unique passcode is sent to a phone to type it to 2-factor prompt.
- **Phone callbacks**; this method will give a phone call to give the needed code to account during logon.
- **TOTP**; this is like SMS, but it will generate time-based one-time passcodes.
- **U2F Device**; this uses USB hardware device and a server. Users taps the device inserted to their USB drive.

3.4 Future

In the future it is possible to extend the 2-factor authentication to cover the entire staff and somedays also the students when they use VPN, Office365 and similar systems. But they are challenges on the way. Especially in Office365 implementation of 2-factor authentication brings things to plan. 2-factor authentication is generally done with the phone, but very often teachers, when teaching in the classroom, leave their phones to their office and do not carry phones with them. If they need to log on to a Office365 cloud resource, they will not be able to sign in if their phone is not near them. Security and ease of use correlate with each other, that is, the safer the system, the more difficult it´s daily use is usually. In SAMK´s case staff should always carry the phone when moving in the campuses and especially if 2-factor authentication is expanding to other major systems.

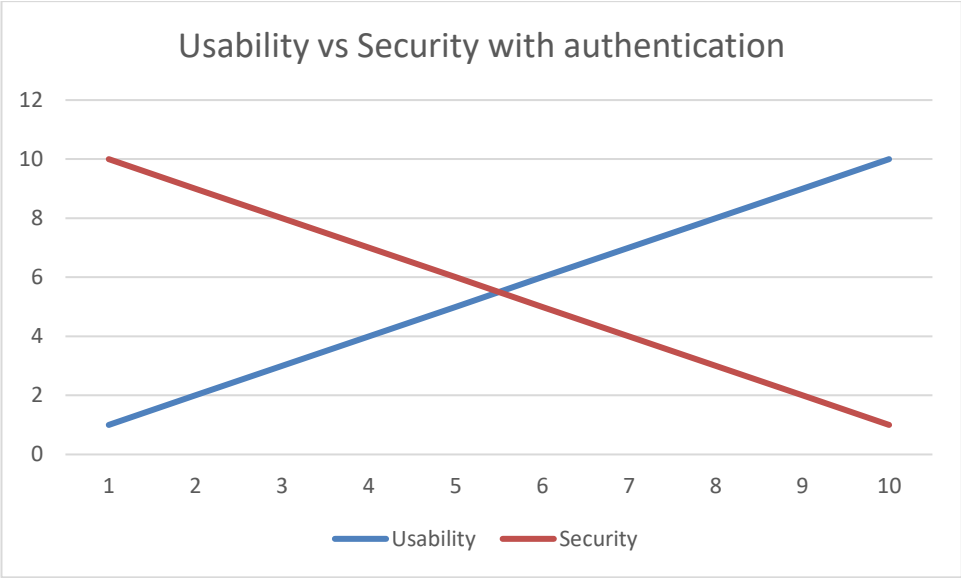
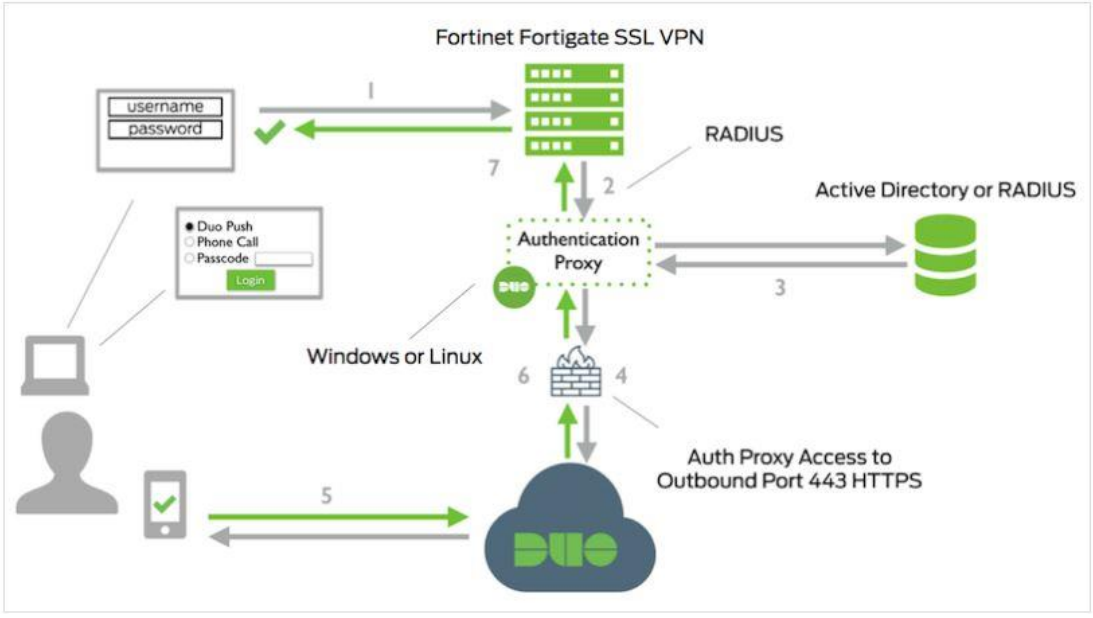


Chart 1. This chart shows Usability vs Security with authentication methods.

4 WORKING WITH THE PROJECT

4.1 Duo Mobile

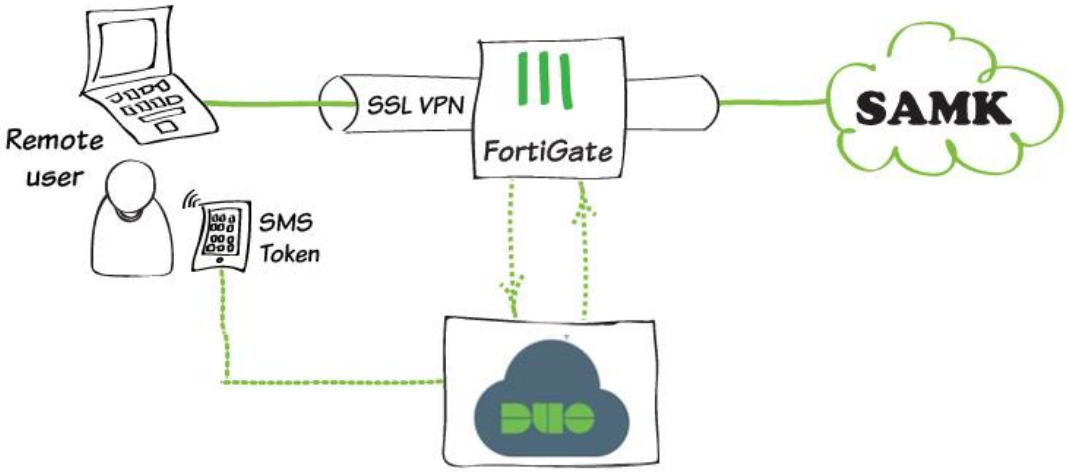
Duo mobile requires a working primary authentication configuration to SAMK FortiGate SSL VPN use. A local proxy server need to be installed to act as a RADIUS server. This proxy will get the authentication and contact Active Directory or RADIUS to check the user and finally communicate to DUO portal, which will then check and send authentication message code or other method to the user. This proxy can be a Windows or Linux server, but this installation will use a Windows 2012 R2 –based server, because DUO recommends it as primary windows server OS.



Picture 5. DUO 2FA (Duo Security Inc., 2018)

The VPN appliance is a Fortinet FortiGate 100D VPN.

Picture 6. Fortinet FortiGate 100D (AVFirewalls.com, 2018)



Picture 7. DUO and SAMK, self-edited picture. (Fortinet Techincal Documentation, 2018)

4.1.1 Authentication proxy server

DUO mobile proxy server requires some configuration. At least it needs to know;

- Radius service / Active Directory domain controller host addresses. Active Directory domain controller will perform primary authentication.
- Service account, which have permission to read Active Directory data.

- Security group or Organizational Unit, from where the users can log on. This is optional.
- DUO mobile secret keys
- DUO mobile service location.
- Radius IP where those sign-ins come (FortiGate VPN address)

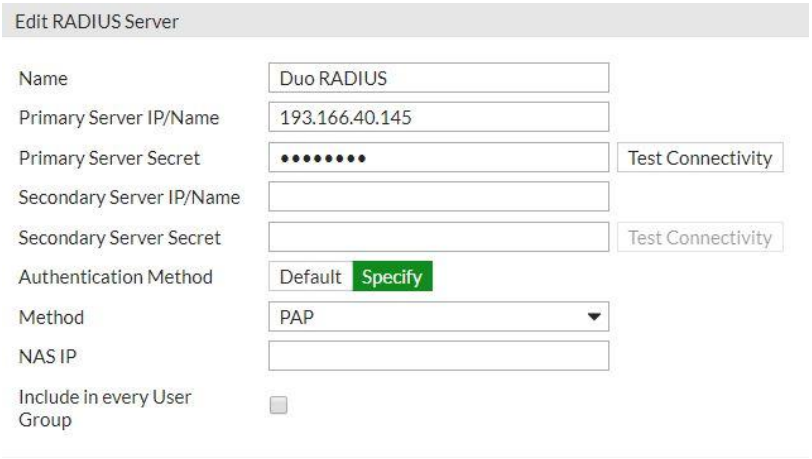
The configuration written to DUO Proxy (authproxy.cfg) server will be like this:

```
[ad_client]
host=193.166.149.121
host_2=193.166.149.120
service_account_username=DuoMobile
service_account_password=**********
search_dn=DC=ad,DC=local

[radius_server_auto]
ikey=DI23CSWHD0MTQ8ZTV9EN
skey=**********************************
api_host=api-db0d50ec.duosecurity.com
radius_ip_1=193.166.40.145
radius_secret_1=sekretti
client=ad_client
port=1812
failmode=safe
```

These options are the minimum required, but there´s much more options to choose if the configuration needs to be more secured. Active Directory-based users can be limited to a group or organizational unit. Transport protocol can be limited to SSL/TLS and then assign a valid certificate for that. The authentication type to use with active directory server can be plain, NTLM version 1 or 2.

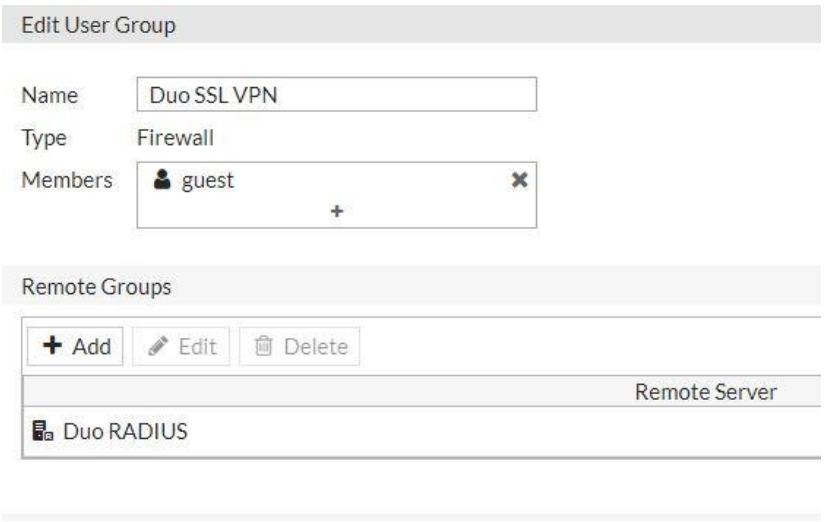
4.1.2 Fortigate 100D setup

In FortiGate VPN controller a RADIUS server must be added. Server address must be the authentication proxy address.



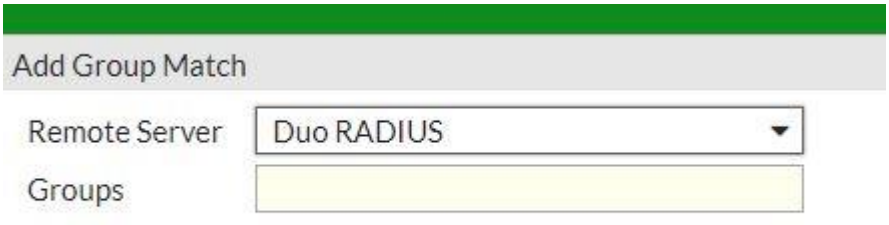
Picture 8: RADIUS server edit menu (Fortigate Inc., 2018)

A new group must be added to FortiGate. When a VPN connection request begins, user is authenticated from RADIUS proxy if that user is configured locally to Forti-Gate.



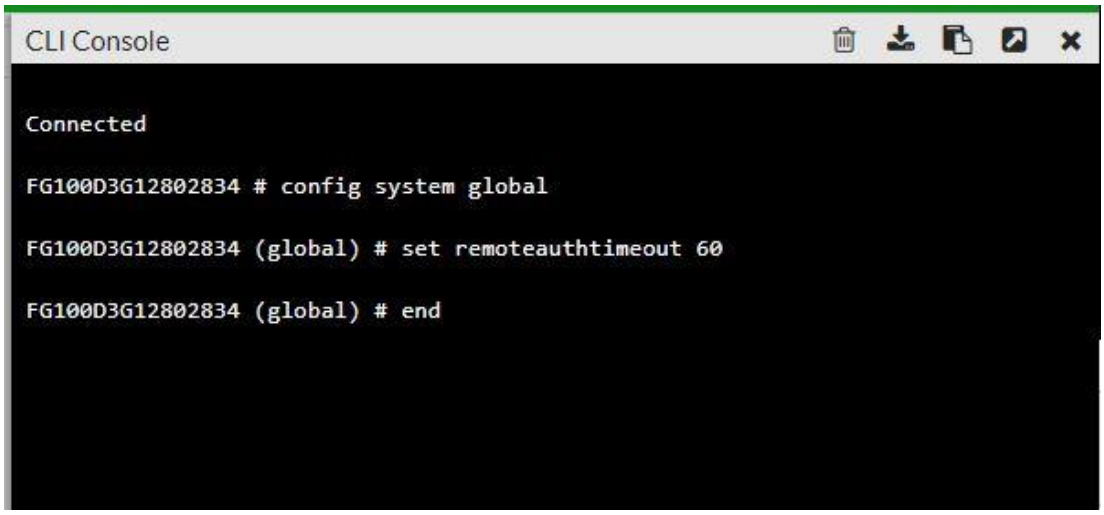
Picture 9: RADIUS address edit menu (Fortigate Inc., 2018)

Duo RADIUS is matched to SSL VPN groups.



Picture 10: RADIUS Group match edit menu. (Fortigate Inc., 2018)

A timeout needs to be configured, because default timeout for FortiGate appliance is 5 seconds and that will cause fail for anything other than a passcode authentication. Timeout need to be increased and DUO recommends at least 60 seconds timeout.



Picture 11: Fortinet CLI console (Fortigate Inc., 2018)

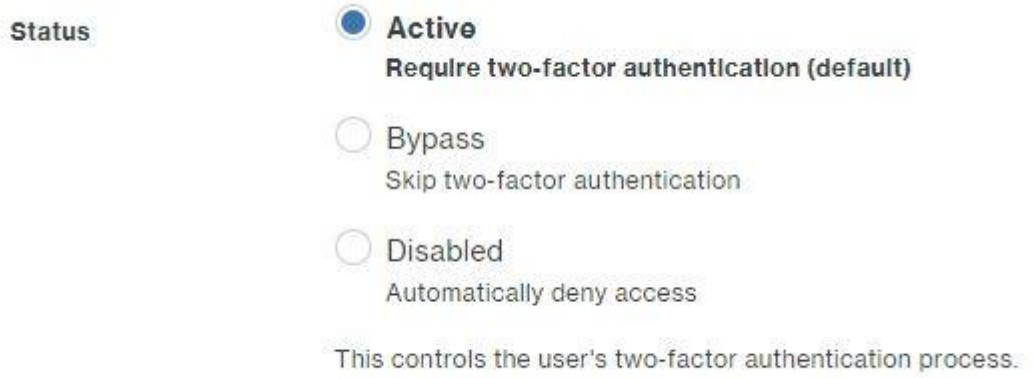
4.1.3 DUO Mobile client setup

DUO Mobile management portal can be attached to active directory service if user registration is wanted to be done automatically or with the self-service. This is an additional feature in DUO and costs extra, because of additional licensing. In SAMK case, the end-user group is so small, so administrator can register users to the service. After registration DUO asks to send a text message to the users so they can finish registration process and connect their mobile phone to DUO service.

Device	Platform	Model	Duo Mobile	Security Warnings	Users
+358 44 7103824	Windows 10 Mobile 10.0.14393.2068	NOKIA RM-984_1005	2.0.4.1	✔ No warnings	jori, jokymal

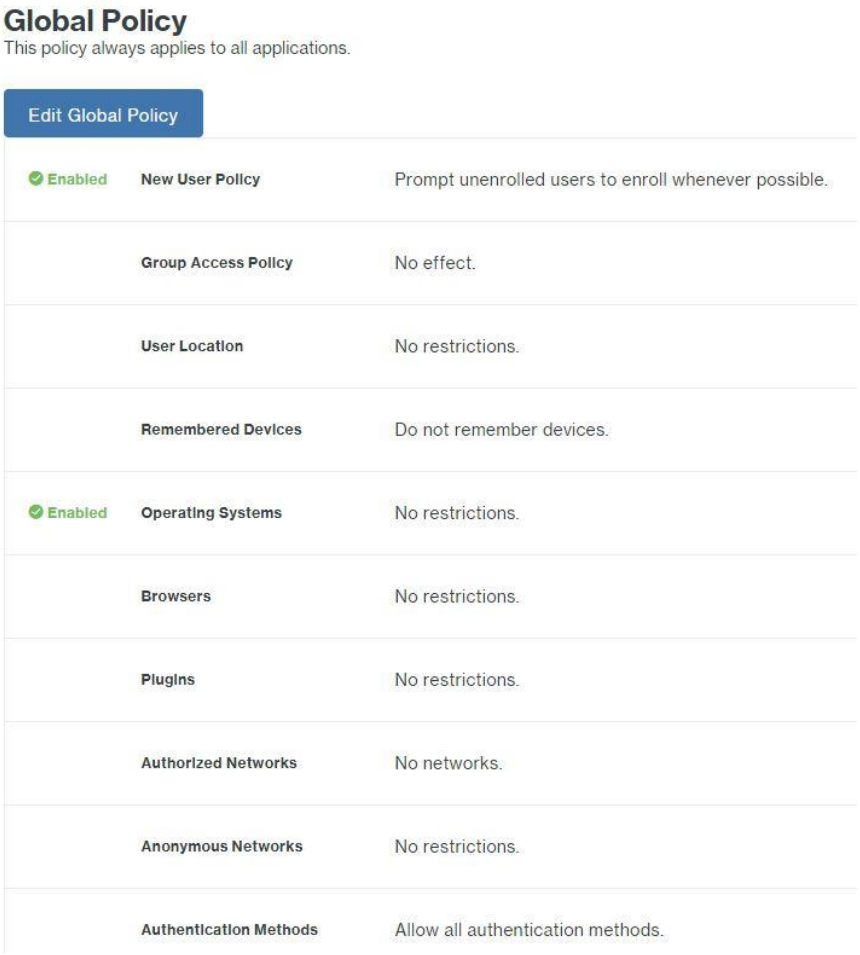
Picture 12 and 13: DUO user portal (Duo Security Inc., 2018)

New users will be automatically activated to 2-factor authentication. If necessary, the users 2-factor authentication can be temporarily bypassed or users 2-factor authentication can be disabled, this will deny access to logon.



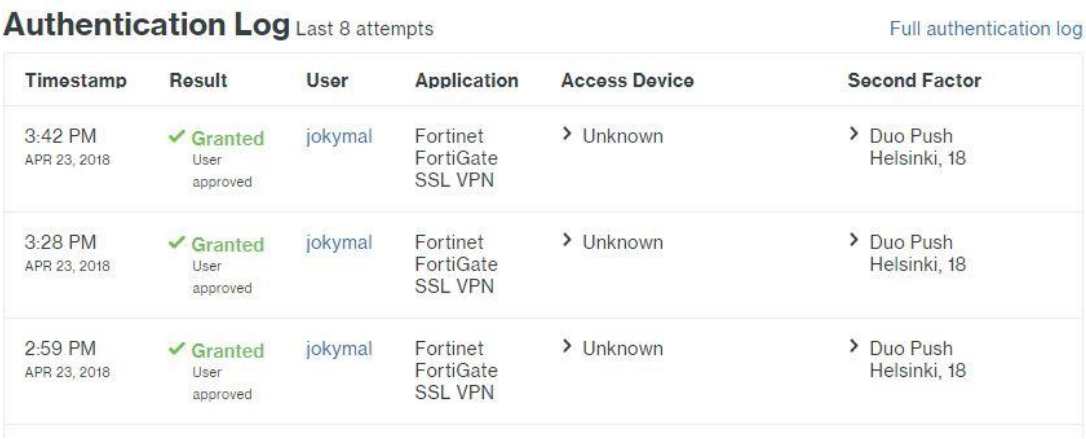
Picture 14: DUO user Status (Duo Security Inc., 2018)

The DUO admin interface has a wide variety of options available for use. It is possible to allow or restrict connection based on operating system, browser, user location or network type. It is therefore possible to make a very precise policy for users if needed.



Picture 15: DUO user policies (Duo Security Inc., 2018)

In the authentication log monitor it is possible to log user activity and authentication functionality as well as the second factor method and location used. DUO Mobile can be switched with multiple authentication environment. FortiGate SSL VPN is just one solution among others.

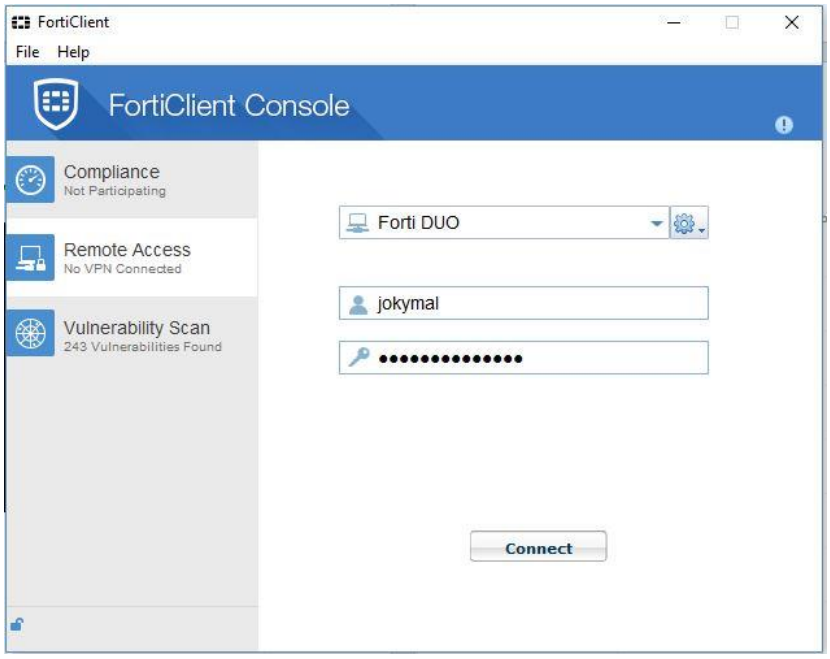


Picture 16: DUO authentication log (Duo Security Inc., 2018)

5 RESULTS

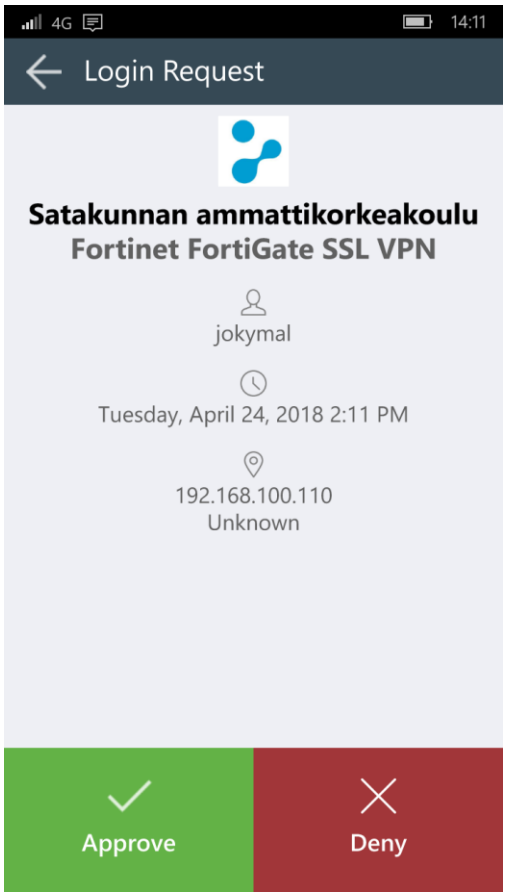
The test environment was built and configured as described in the previous section. At the beginning of the test, the access rules and permissions in the VPN appliance had to be adjusted and reconfigured several times and that did some extra job. At last the test environment passed all checks and the testing of sign-in to SSL VPN and its 2-factor authentication could begin.

FortiGate forticlient was downloaded and installed. In the configuration section the connection to test environment was named “Forti DUO”. User account is the real active directory account, because the authentication checks credentials from SAMK production AD environment.



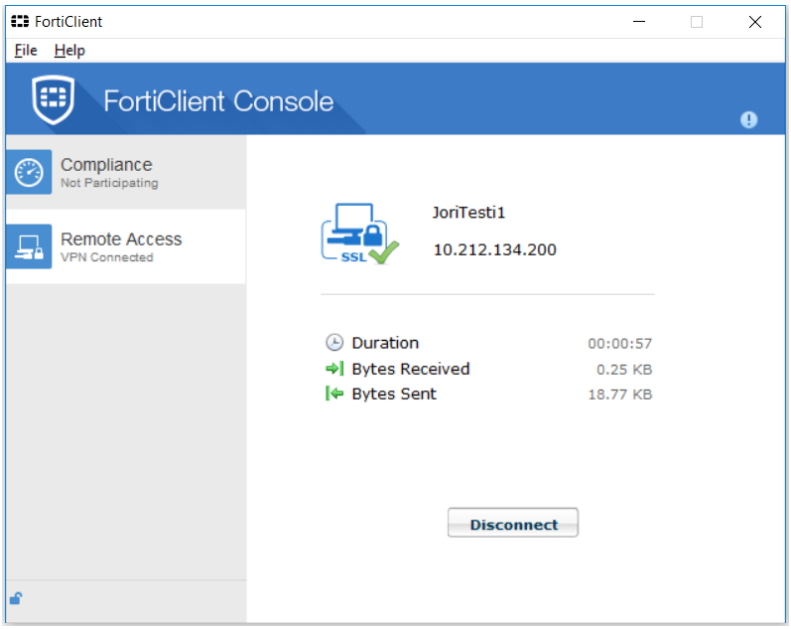
Picture 17: FortiGate SSL VPN Client (Fortigate Inc., 2018)

When logon process began, DUO Mobile client activated and asked to approve the logon request. In this lab no SMS or passcode was used, 2-factor authentication was configured to approve or deny logon request in the mobile application.



Picture 18: DUO Mobile application (Duo Security Inc., 2018)

Once authentication was accepted, Forticlient continued the sign-in process and the VPN tunnel opened. User could now start working normally and was VPN secured.



Picture 19: Authentication granted, FortiGate SSL VPN (Fortigate Inc., 2018)

When all challenges were resolved and the hardware and environment configuration was completed, test environment could begin use 2-factor authentication in VPN. The outcome result was desired. Now this environment can also be applied to 2-factor based authentication, such as management networks used by administrators. The environment can also be extended to all SAMK users, but then DUO licensing models and additional services must be checked. Depending on licensing model, more options are available, which can benefit the larger number of users and users of different skills.

The results of this case study are not related only to SAMK environment, but similar functionalities and tests can be applied to other environments as DUO Mobile is flexible in various solutions and requirements. The SAMK environment tests can also be introduced to other organizations that might be interested about the use of 2-factor authentication. Especially in the academic world, there may be interests in this, as knowledge and usage experiences are widely exchanged between the universities of applied sciences.

6 CONCLUSIONS

Two-factor authentication brings one extra extension to traditional authentication. This authentication method requires that two of these factors must be fulfilled:

- Something you know
- Something you have
- Something you are

Quite often this is done by password and mobile phone. Users puts credentials when logging on to a service and 2-factor service sends SMS or mobile code to user smartphone and that is a pass to continue the logon process. Banks have user multi-factor authentication for a long time and nowadays many web services can be implemented with two-factor or multifactor authentication layer especially because it is easy to implement in cloud-based services and they are growing hugely.

Enterprise environments need better security, so implementing more authentication factors to these environments raises security especially in critical services, where hacking can lead to catastrophic consequences. There are many authentication services that can connect to enterprise environments and user data, if authentication information is not able or not wanted to take from cloud-based services.

6.1 Case SAMK

Two-factor authentication was tested in Satakunta University of Applied Sciences environment with the FortiGate VPN solution and DUO Mobile authentication service. The test succeeded well and showed, that it is possible to implement this solution to ICT administration and, if needed, expand it to more extensively to other staff depending on the usage needs. At first 2-factor authentication use will start in the management systems used by ICT administrators.

Some of the services used in SAMK environment are already ready to switch with two-factor e.g. Office365, but this requires a somewhat larger amount of monetary

inputs and more connections to Microsoft Azure cloud. In addition, staff should be accustomed to different everyday use and they must start to keep their phone with them in classrooms and where they may need to logon to their wide used applications.

6.2 Future

When implementing two-factor authentication system in an environment, some questions need to be asked. If not controlled, two-factor authentication may be a major cost to organization. Even if it is strongly implemented with legacy systems.

- How will the system cope with future trends?
- Will the system scale with numbers of users?
- Is there capability to introduce new functionality to address new threats?
- How are tokens (if not using mobile apps) to be issued and reissued to end-users.
- Is Helpdesk facilities capable to deal with authentication issues?

Two-factor authentication is more powerful than traditional authentication based only to username and password, but also opens new threats to various security breaches such as forgetting or stealing smartphones or security tokens. Must the authentication efficiency be changed to higher protection? Biometric authentication in addition to 2-factor authentication or additional authentication e.g. 3- or 4-factor authentication. Efficiency and convenience are usually in reverse order, as described earlier in this thesis. Users do not easily take more secure practices than they feel useful. In business environments this practice is more based to organizations security policy, not on user behavior. The user may disagree with the company´s security department, but at work, the company´s security policy must be respected.

REFERENCES

Amazon Web Services. (2018, April 20). *AWS Webcast - Securing the Microsoft Windows Platform on Amazon Web Services*. Retrieved from SlideShare: https://www.slideshare.net/AmazonWebServices/aws-webinar-msftsecdec2013

AVFirewalls.com. (2018, April 30). *Fortinet FortiGate 100D*. Retrieved from AVFirewalls Fortinet Authorized Online Reseller: http://www.avfirewalls.com/FortiGate-100D.asp

Duo Security Inc. (2018, April 23). Pori, Satakunta, Finland.

Duo Security Inc. (2018, April 23). *DOCUMENTATION Fortinet FortiGate SSL VPN*. Retrieved from Duo: https://duo.com/docs/fortinet?ikey=DI23CSWHD0MTQ8ZTV9EN&host=api-db0d50ec.duosecurity.com#eyJoYXNoIjoiIiwic2VhcmNoIjoiP2lrZXk9REkyM0NTV0hEME1UUThaVFY5RU4maG9zdD1hcGktZGIwZDUwZWMuZHVvc2VjdXJpdHkuY29tIn0=

Duo Security Inc. (2018, April 23). *Secure Access Starts With (Zero) Trust*. Retrieved from DUO: https://duo.com/

Fortigate Inc. (2018, April 24). Pori, Satakunta, Finland.

Fortinet Techincal Documentation. (2018, April 30). *SMS two-factor authentication for SSL VPN*. Retrieved from The Fortinet Cookbook: http://cookbook.fortinet.com/sms-two-factor-authentication-ssl-vpn/

Google inc. (2018, April 20). *Securing your Cloud Platform Account with Security Keys*. Retrieved from Google Cloud: https://cloud.google.com/solutions/securing-gcp-account-security-keys

Hammond, M. &. (2013). *Research methods: The key concepts*. London; New York: Routledge.URL.

Komonen, O. (2017, June 7). *Tiukat turva-asetukset suojaavat Google-tiliäsi – näin ne ohitetaan vaivatta*. Retrieved from Tivi: https://www.tivi.fi/Kaikki_uutiset/tiukat-turva-asetukset-suojaavat-google-tiliasi-nain-ne-ohitetaan-vaivatta-6655504?utm_source=Tivi_Uutiskirje&utm_medium=email&utm_campaign=Tivi_Uutiskirje

Microsoft Corporation. (2018, April 20). *How Azure Multi-Factor Authentication works*. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Millett, S. T. (2003). *Who Goes There? Authentication Through the Lens of Privacy.* Washington, D.C.: THE NATIONAL ACADEMIES PRESS.

Rosenblatt, S., & Cipriani, J. (2015, June 15). *Two-factor authentication: What you need to know (FAQ)*. Retrieved from CNET: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

Santamäki, O. (2018, April 27). (J. Kymäläinen, Interviewer)

Thomson, I. (2018, January 17). *Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication*. Retrieved from The Register: https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/

Thomson, I. (2018, January 17). *Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication*. Retrieved from The Register: https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/

U.S. Department of Commerce. (2018, April 20). Retrieved from Technology, National Institute of Standards and Technology: https://www.nist.gov

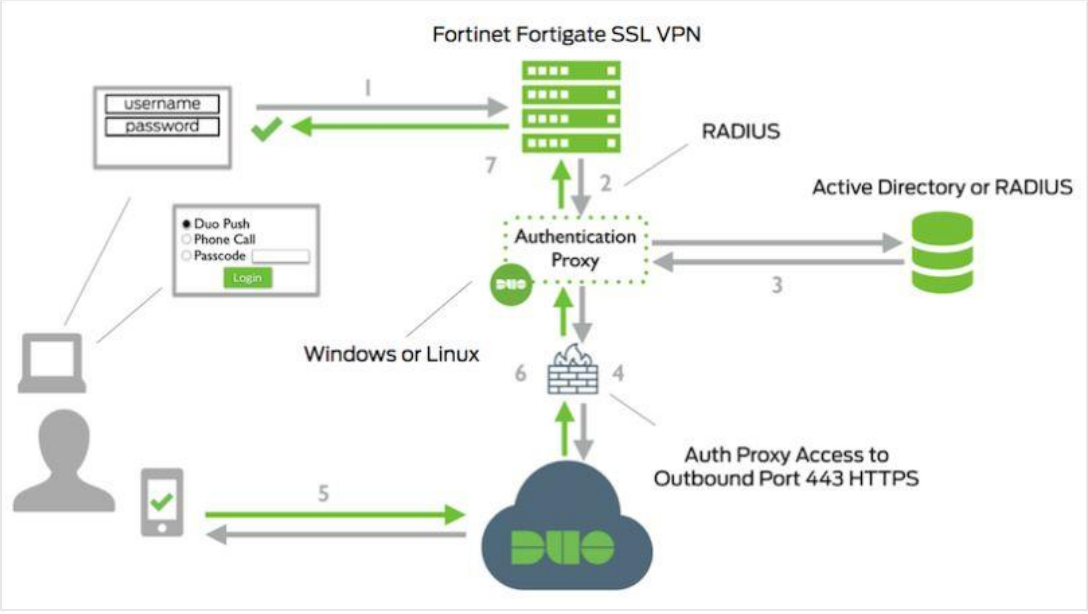
APPENDIX 1

DUO MOBILE 2-VAIHEISEN AUTENTIKOINNIN KONFIGURAATIO JA KÄYTTÖÖNOTTO

Tässä dokumentissa on kerrottu, kuinka DUO Mobilen 2-vaiheinen tunnistautuminen on kytketty FortiGate SSL VPN -järjestelmän kautta tarvittavaan kirjautumiseen. Dokumentissa toteutetaan kirjautuminen administratiivisiin järjestelmiin, jolloin käyttäjämäärä on pieni eikä DUO:ta tarvitse kytkeä AD-ympäristöön. Lisäksi käyttäjiä on alle 10kpl, joten standardein lisenssi riittää (ilmainen). Järjestelmän ja tarpeiden kasvaessa pystytään toimintaa laajentamaan.

Huomioi nämä ohjeen sisältymättömät seikat käyttöönotossa:

- FortiGate pitää olla määritelty ja testattu niin, että käyttäjä saa sillä luotua perinteisen VPN-yhteyden. Tässä vaiheessa vain testataan, että VPN-ratkaisu itsessään on oikein määritelty.
- Palomuurista on auki tarvittavat yhteydet DUO Mobile-palvelun ja Radius Proxy-palvelimen välillä.
- Windows Server 2012 R2-serveri (tai Linux, mutta ohje on Windowsille). Ei tarvi olla kiinni domainissa, mutta oltava pääsy AD-verkkoon ja ulkomaailmaan DUO-palveluun. AD:n DC hoitaa primäärin autentikoinnin. Kannattaa kokeilla myös 2016 serverillä.
- Service-tunnus, jolla on oikeus lukea AD:n attribuutteja. Normaali User riittää.



DUO MOBILE

1. www.duo.com -osoitteessa luo käyttäjätunnus ja kysyttäessä valitse 10-userin free-versio.
2. Applications-valikossa luo uusi applikaatio. Valitse listalta ”Fortinet FortiGate SSL VPN”. Applikaation tullessa luoduksi sivuilla näkyy ”See the Fortinet Documentation…” -linkki, mutta sitä ei voi laittaa tähän, koska linkin osoite ei ole vakio. Siellä on syvällisempi ja uusin dokumentaatio.
    a. Integration key
    b. Secret key
    c. API hostname, tallenna nämä kolme arvoa ylös, niitä tarvitaan proxyn määrittelyssä.
3. Global Policy -kohdan voi jättää oletuksena määrittelemättä, mutta tuotantokäytössä kannattaa kiinnittää huomiota ko. policyihin, ne tarjoavat hyvin monta hyödyllistä räätälöintimahdollisuutta. Palvelu toimii heti, vaikka kaikki muu ko. valikossa olisi jätetty oletusarvoihin.
4. Save changes

Luo käyttäjä

5. Users-valikossa luo samanniminen käyttäjä, kuin mikä vastaava on AD:n käyttäjätunnuksen nimenä. Tämä tehdään näin, koska käyttäjät ylläpidetään DUO-palvelussa. Muuten kytkettäisi AD:hen (optio). Status = aktiivinen
Luontivaiheessa kysytään, lähetetäänkö käyttäjälle SMS-viestillä DUO:n aktivointilinkki. Vastaa kyllä. Käyttäjä saa linkit DUO-applikaation lataukseen ja aktivointiin. Nämä käyttäjän täytyy suorittaa, ennen kuin 2fa alkaa pelaamaan.

RADIUS PROXY

6. Asenna Windows 2012 R2-palvelin perusasetuksineen. Minimivaatimus on 1 CPU, 200Mb levyä, 4Gb RAM (jopa 1 riittää). Ei liitetä AD:hen. Lataa ja asenna Authentication proxy: https://dl.duosecurity.com/duoauthproxy-latest.exe
7. Mene palvelimella osoitteeseen
64-bit: C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg
Linux: /opt/duoauthproxy/conf/authproxy.cfg

    Syötä seuraavat rivit (vähimmäisvaatimus, DUOn konfigurointiohjeissa on huomattavasti enemmän optioita, jos halutaan mm. OU-tasolla sallinnat ym.). Kommentteja ei tule syöttää.

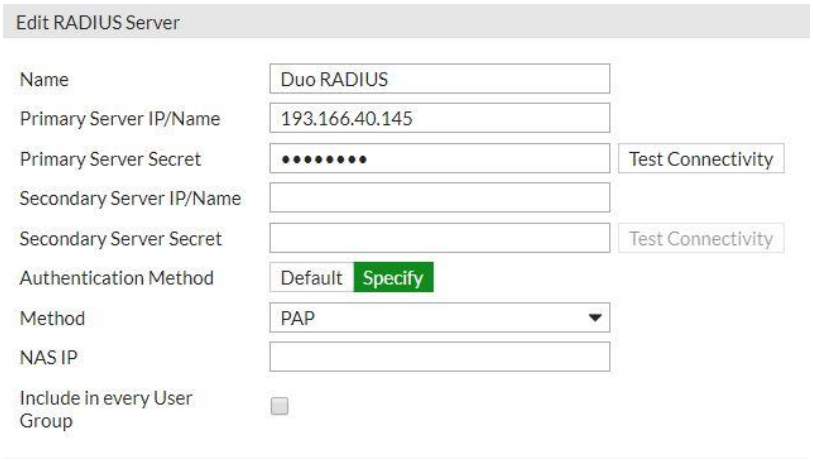
```
[ad_client]

host=193.166.149.121  Kommentti:DC:n osoite

host_2=193.166.149.120    Kommentti: vaihtoehtoisen DC:n osoite
```

```
service_account_username=DuoMobile   Kommentti: AD:n service-tunnus, user-
tasoinen

service_account_password=**********  Kommentti: salasana selkotekstillä

search_dn=DC=ad,DC=local   Kommentti: ad:n polku. Optioilla voi laittaa OU-
tasollekin.


[radius_server_auto]

ikey=DI23CSWHD0MTQ8ZTV9EN   Kommentti: Katso nämä DUO:n applications-
valikosta.

skey=**********************************  Kommentti: Syötettävä selkokielellä

api_host=api-db0d50ec.duosecurity.com  Kommentti: Ks.DUO

radius_ip_1=193.166.40.145  Kommentti: FortiGaten IP, johon proxyllä on pääsy.

radius_secret_1=sekretti   Kommentti: keksi tämä itse, täytyy syöttää
FortiGateenkin.

client=ad_client  Kommentti: RADIUS-palvelu on AD:ssa kiinni.

port=1812   Kommentti: Optio, oletusportti Radiukselle 1812, mutta voi antaa
muunkin.

failmode=safe  Kommentti: Optio, jos radius feilaa, 2fa ohitetaan eli
kirjautua pystyy.
```

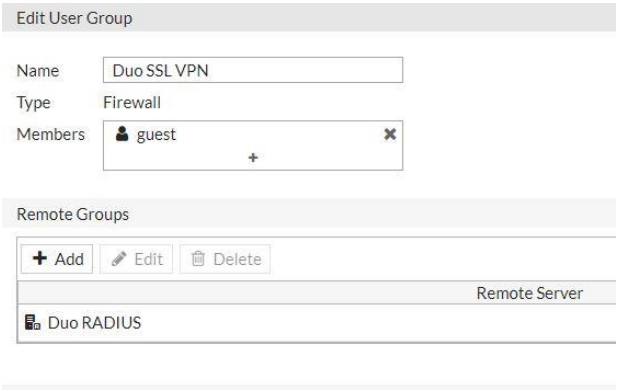
8. Kun olet tehnyt tarvittavat asetukset kuntoon, tallenna ja sulje tiedosto ja käynnistä proxy-service. CMD:llä ”net start DuoAuthProxy”.
    a. Jos teet muutoksia fileen, muista uudelleen käynnistää proxy service aina muutosten jälkeen; ”net stop DuoAuthProxy” & ”net start DuoAuthProxy”.

FortiGate -laite

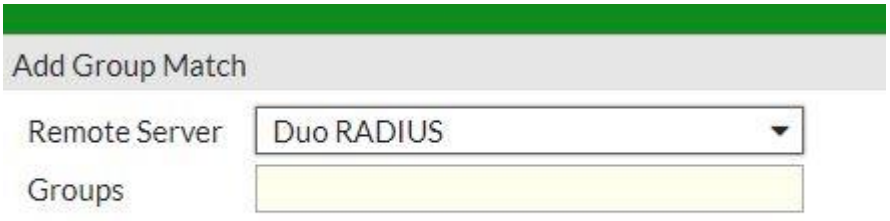
9. Valikoiden nimet ja sijainnit vaihtelevat hieman riippuen laitteiston mallista ja firmware-versiosta.
    a. Nimeksi Duo RADIUS.
    b. Typeksi Query
    c. RADIUS-serverin edit-menuun syötä Primary server IP:ksi ed. kappaleessa luodun Proxy-palvelimen IP, johon FortiGatella on pääsy.
    d. Primary Server Secretiin anna proxyssa kirjoittamasi secret.
    e. Test Connectivityn pitäisi mennä läpi. Koita esim. jollain AD-tunnuksella, kuten service-tunnuksella.
    f. Authentication Method tulee Specify-valikon takaa löytyvä PAP.



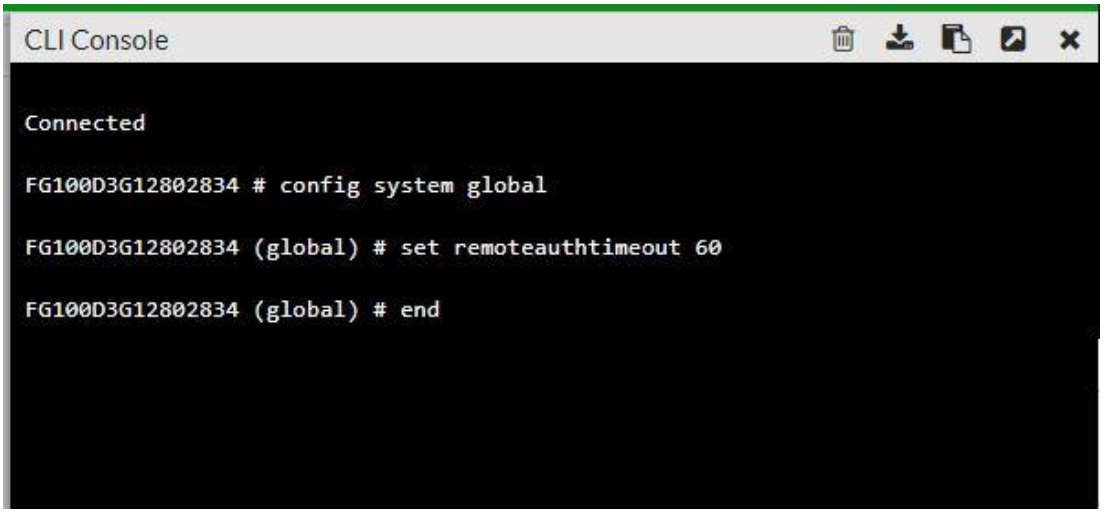
10. FortiGaten User Groupeissa luo uusi Group tai editoi olemassa olevaa Groupia. Jos uusi;
    a. Group nameksi: Duo SSL VPN
    b. Type: Firewall



11. Add Group Matchissa lisää remote serveriksi Duo RADIUS.



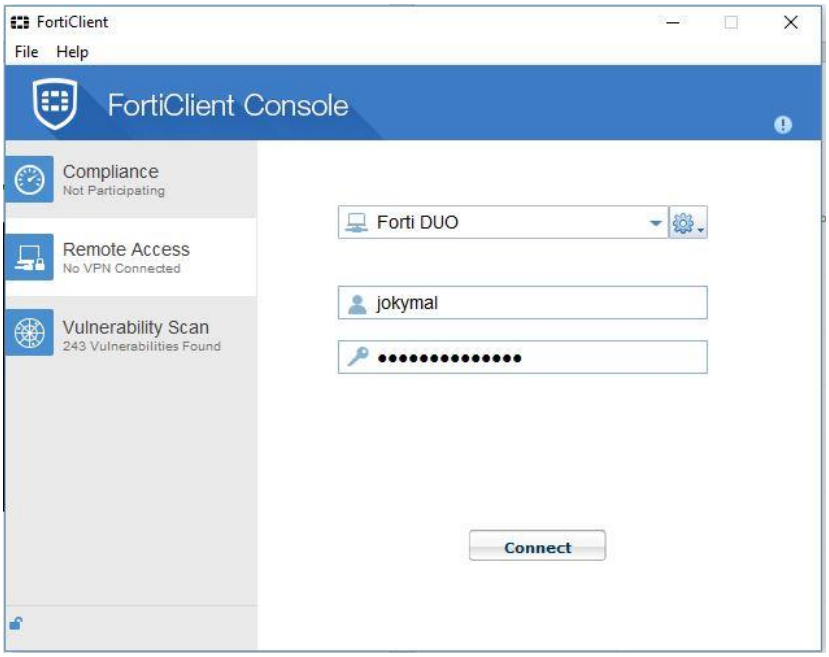
12. FortiGatessa default timeout on 5 sekuntia, mikä on liian lyhyt aika 2fa:lle eli käytännössä vain passcode authentication toimisi. Siis kasvatetaan timeout 60 sekuntiin. Tämä tehdään Command-line-interfacessa eli CLI:ssä. Löytyy yleensä FortiGaten hallintakonsolissa oik. yläkulmasta.



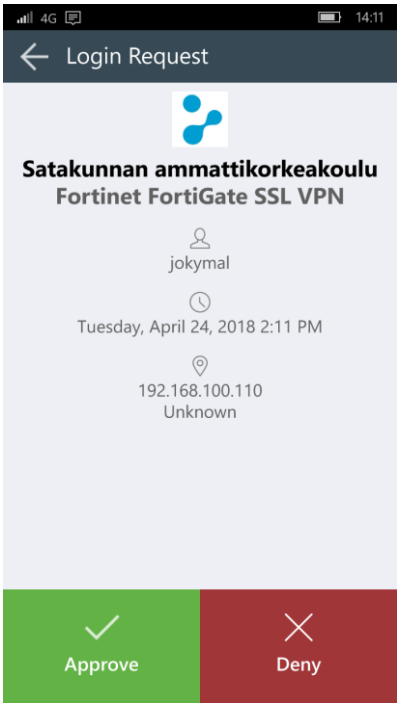
13. Nyt kaiken peruskonfiguraation pitäisi olla kunnossa ja pääset kokeilemaan yhteyttä.

YHTEYSKOKEILU

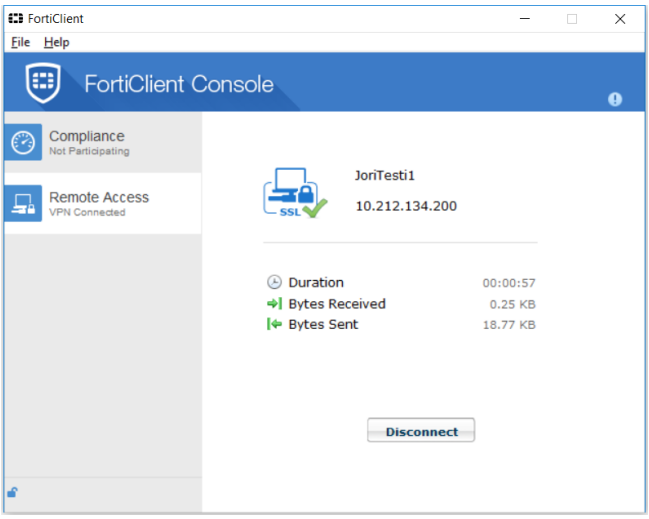
14. Asenna/avaa työasemalle FortiClient ja konfiguroi siihen VPN-yhteys FortiGateen.



Kun logon-prosessi alkaa, pitäisi kirjautumisen pysähtyä ja kännykkäsi ilmoittaa, että DUO Mobilessa on uusi Login request. Hyväksy request painamalla APPROVE-valintaa.



15. Jos kaikki meni hyvin, logon jatkuu ja näet lopuksi yhteyden muodostumisesta kertovan ikkunan.



Tämän dokumentin mukaan suoritettu asennus on vain perusasennus, joilla hommassa pääsee alkuun ja se soveltuu lähes sellaisenaan ylläpidon käyttöön. Lopullisessa käyttöönottoasennuksessa tai autentikoinnin laajetessa koskemaan isompaa käyttäjäryhmää tulee tutkia myös optiot ja mahdolliset lisenssilaajennukset ja dokumentoida/päivittää tätä dokumenttia ajanmukaiseksi. Tehdyt lisäykset kannattanee lisätä tämän dokumentin loppuun, jotta perusasennusohje ei mene sekaisin ja runko säilyy validina.